UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/942,633	08/30/2001	Steven Black	AUS920010244US1	8760

7590 10/27/2005

Duke W. Yee
Carstens, Yee & Cahoon, LLP
P.O. Box 802334
Dallas, TX 75380

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 10/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/942,633	BLACK ET AL.	
	Examiner	Art Unit	
	Abdulhakim Nobahar	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 August 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,11-17,21-27 and 31-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7,11-17 and 21-27* is/are rejected.

7)☒ Claim(s) *31-39* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Response to Arguments

1. This communication is in response to applicants' amendment received on August 16, 2005.

2. Amendments to claims 1-7, 11, 14, 17 and 21 are acknowledged.

3. Addition of new claims 31-39 are acknowledged.

3. Applicant's arguments with respect to the rejections of claims 1-7, 11-17 and 21-27 under 35 USC § 102 have been fully considered and are persuasive. Therefore, the rejections have been withdrawn. However, upon further consideration, a new ground(s) of rejection necessitated due to applicants amendment of claims.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical

Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1-7, 11-17 and 21-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Porras et al. (6,321,338 B1; hereinafter Porras).

Regarding claims 1, 11 and 21, Porras discloses:

in a first correlation server in a hierarchy of correlation server, logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute (see for example, col. 2, lines 1-10; col. 3, lines 15-41; col. 3, lines 55-65; col. 5, lines 15-64, where the source and destination addresses are the attributes);

classifying events as groups by aggregating events with at least one attribute within the event set as an identical value (see for example, col. 5, lines 15-64; col. 7, lines 5-23, where the source and destination addresses are the attributes);

calculating a respective severity level for each of the groups (see, for example, col. 6, line 52-col. 7, line 3, where the distribution of recently observed values corresponds to the recited calculating a respective severity level);

calculating a delta severity for each group from the respective severity level and a respective prior severity level (see, for example, col. 6, line 52-col. 7, line 3, where

obtaining a score of the event which is an indication of deviation between the short-term and long-term profiles values related to the event corresponds to the recited calculating a delta severity); and

for each group having non-zero delta severity, propagating the respective delta severity to a higher-level correlation server (see, for example, col. 4, lines 61-65; col. 5, lines 30-36; col. 6, line 52-col. 7, line 3; col. 7, lines 4-30, where score threshold corresponds to the recited non-zero delta severity which is being transmitted to the network monitor that corresponds to the recited a higher-level correlation server).

Regarding claims 2, 12 and 22, Porras discloses:

The computer-implemented method of claim 1, wherein the severity levels are calculated based on at least one of the number of event sets within each of the groups, the source attribute of the event sets within each of the groups, the target attribute of the event sets within each of the groups, and the event category attribute of the event sets within each of the groups (see, for example, col. 5, lines 4-64).

Regarding claims 3, 13 and 23, Porras discloses:

The computer-implemented method of claim 1, wherein the events include at least one of a web server event, an electronic mail event, a Trojan horse, denial of service, a virus, a network event, an authentication failure, and an access violation (see, for example, col. 4, lines 31-47; col. 5, lines 25-30).

Regarding claims 4, 14 and 24, Porras discloses:

The computer-implemented method of claim 1, further comprising:

calculating the threshold value based on at least one of the source attribute of the event sets within the group, the target attribute of the event sets within the group, the event category attribute in each event set of the group, and the number of attributes in each event set of the group that are held constant across all of the event sets in the group (see, for example, col. 5, lines 4-64; col. 6, line 52-col. 7, line 3).

Regarding claims 5, 15 and 25, Porras discloses:

The computer-implemented method of claim 1, wherein the target attribute represents one of a computer and a collection of computers (see, for example, col. 1, lines 36-41; col. 2, lines 45-50; col. 5, lines 10-15).

Regarding claims 6, 16 and 26, Porras discloses:

The computer-implemented method of claim 1, wherein the source attribute represents one of a computer and a collection of computers (see, for example, col. 1, lines 36-41; col. 2, lines 45-50; col. 4, line 61-col. 5, line 10-15).

Regarding claims 7, 17 and 27, Porras discloses:

The computer-implemented method of claim 1, further comprising: aggregating a subset of the groups into a combined group (see, for example, col. 7, lines 16-23).

Allowable Subject Matter

Claims 31-39 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US Patent No. 6,779,031 B1 to Picher-Dempsey.

US Patent Pub. No. 2002/0019945 A1 to Houston et al.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abdulhakim Nobahar
Examiner
Art Unit 2132 A. N.

October 20, 2005

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100